Docket: 2480.0015

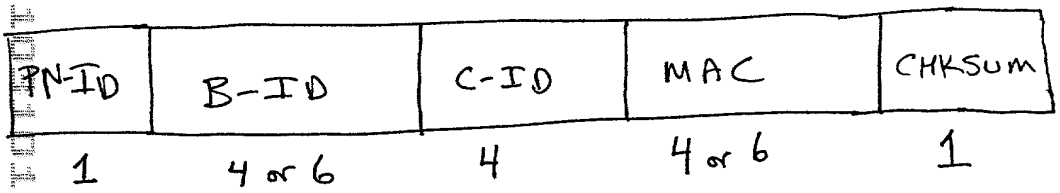


FIG. 1 PRIOR ART

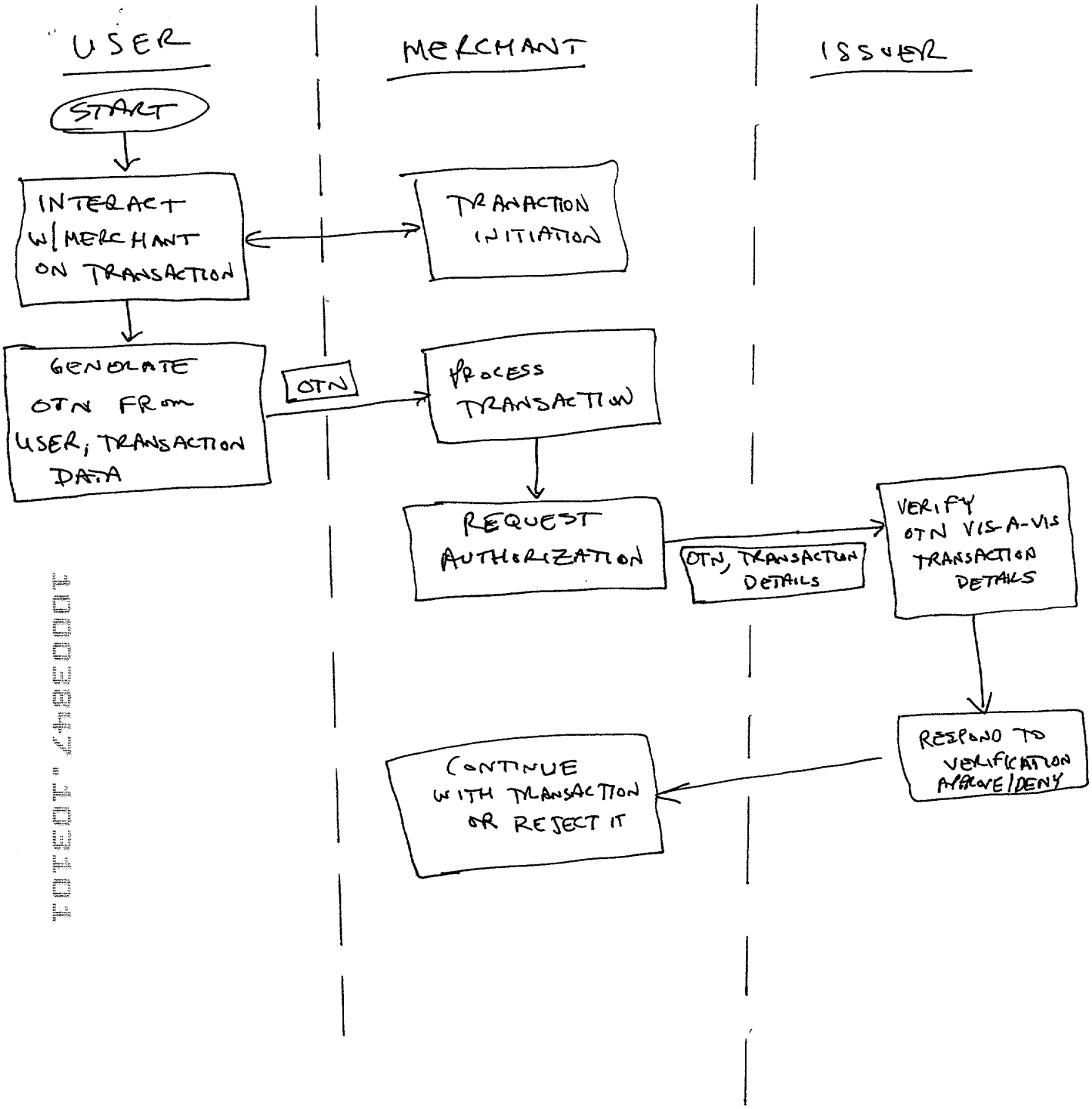


FIG. 2 PRIOR ART

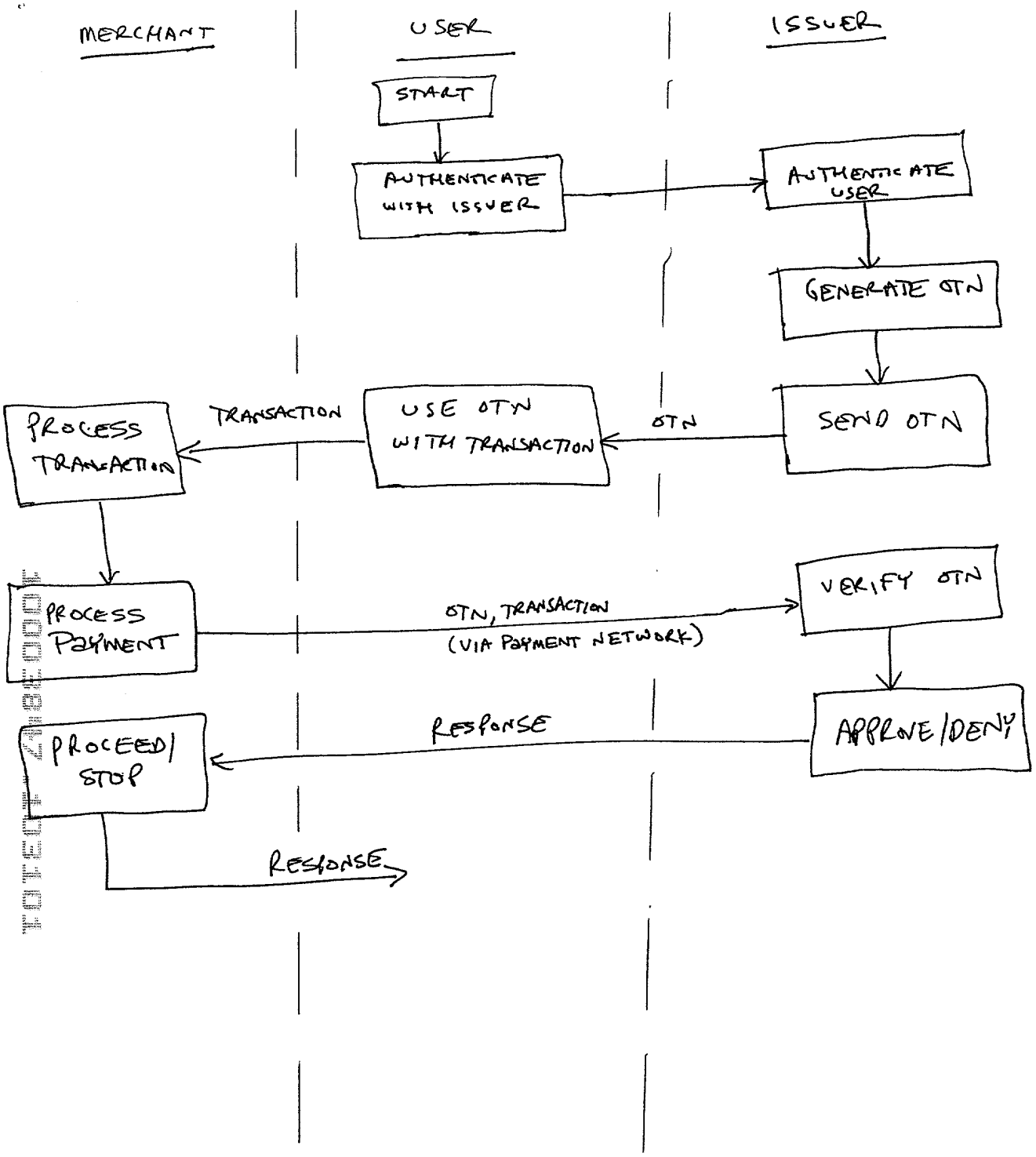


FIG. 3 PRIOR ART

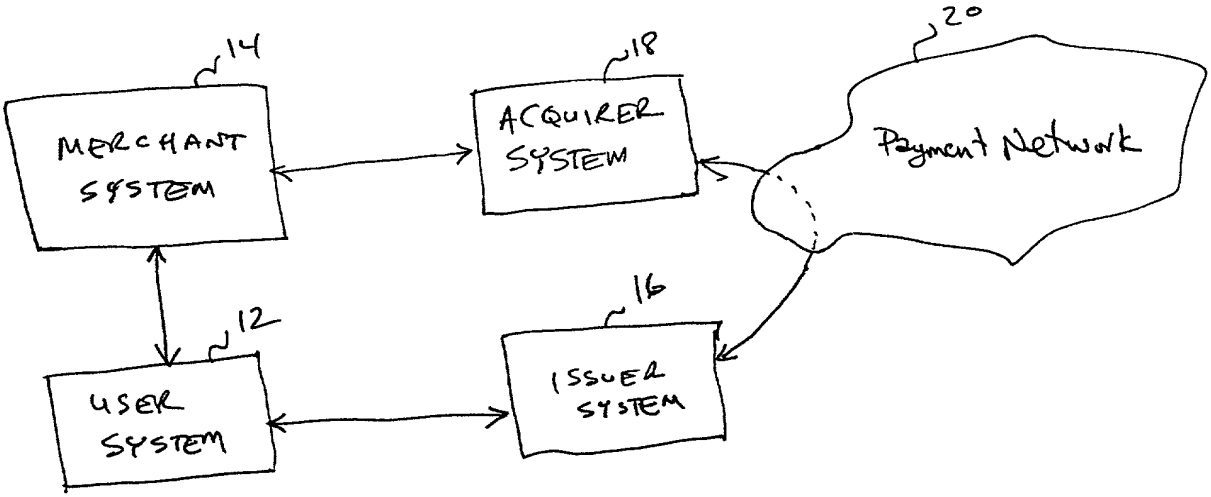
14
MERCHANT SYSTEM
18
ACQUIRER SYSTEM
20
Payment Network
12
USER SYSTEM
16
ISSUER SYSTEM

FIG. 4

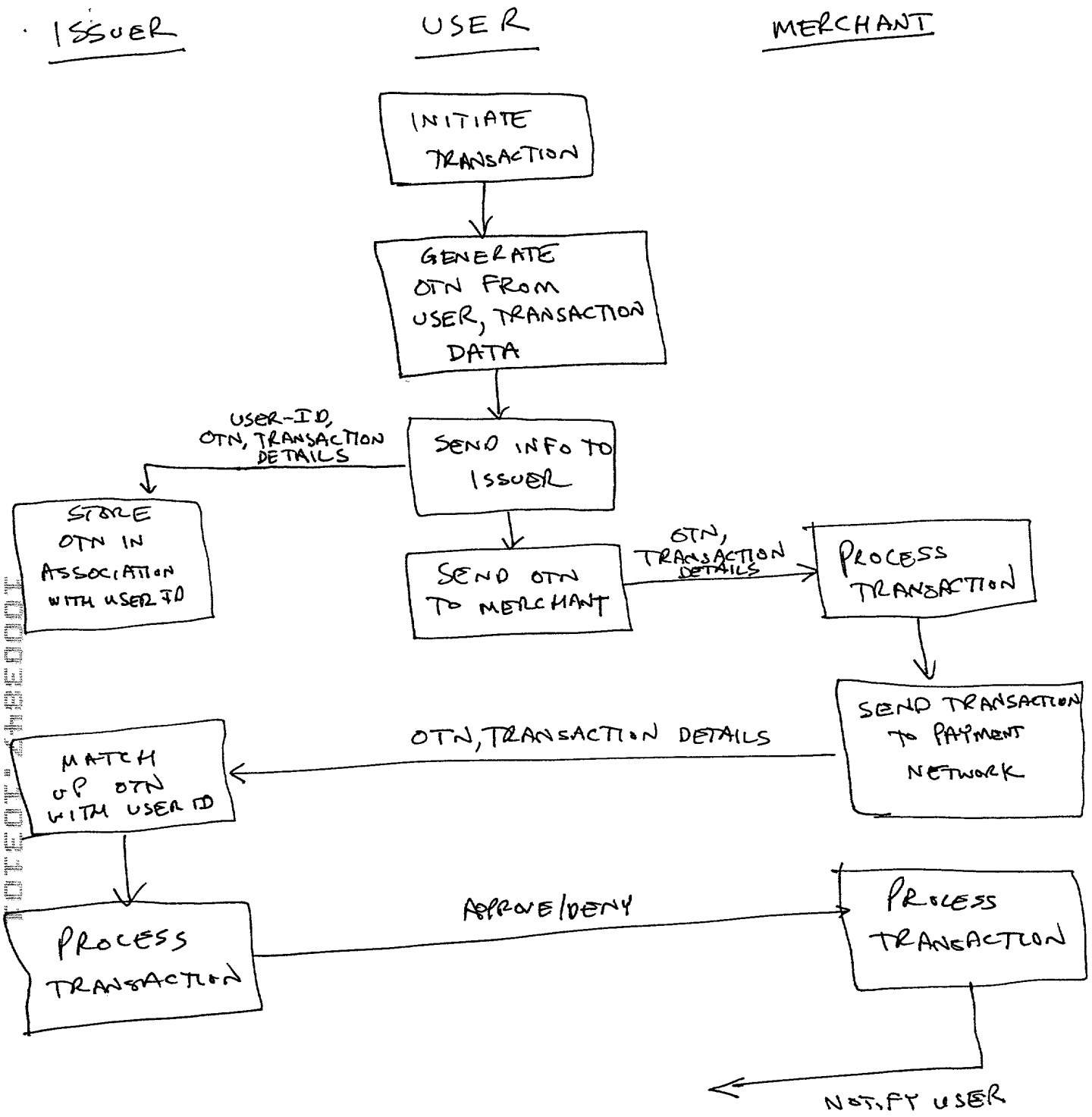
ISSUER
USER
MERCHANT
INITIATE TRANSACTION
GENERATE OTN FROM USER, TRANSACTION DATA
USER-ID, OTN, TRANSACTION DETAILS
SEND INFO TO ISSUER
STORE OTN IN ASSOCIATION WITH USER ID
SEND OTN TO MERCHANT
OTN, TRANSACTION DETAILS
PROCESS TRANSACTION
SEND TRANSACTION TO PAYMENT NETWORK
OTN, TRANSACTION DETAILS
MATCH UP OTN WITH USER ID
PROCESS TRANSACTION
APPROVE/DENY
PROCESS TRANSACTION
NOTIFY USER

FIG. 5

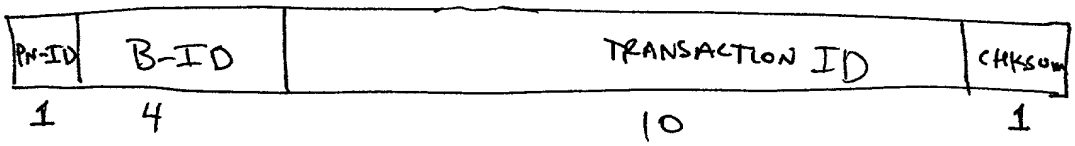


FIG. 6

1.0.0.2.0.T. 7/4/2:00:04

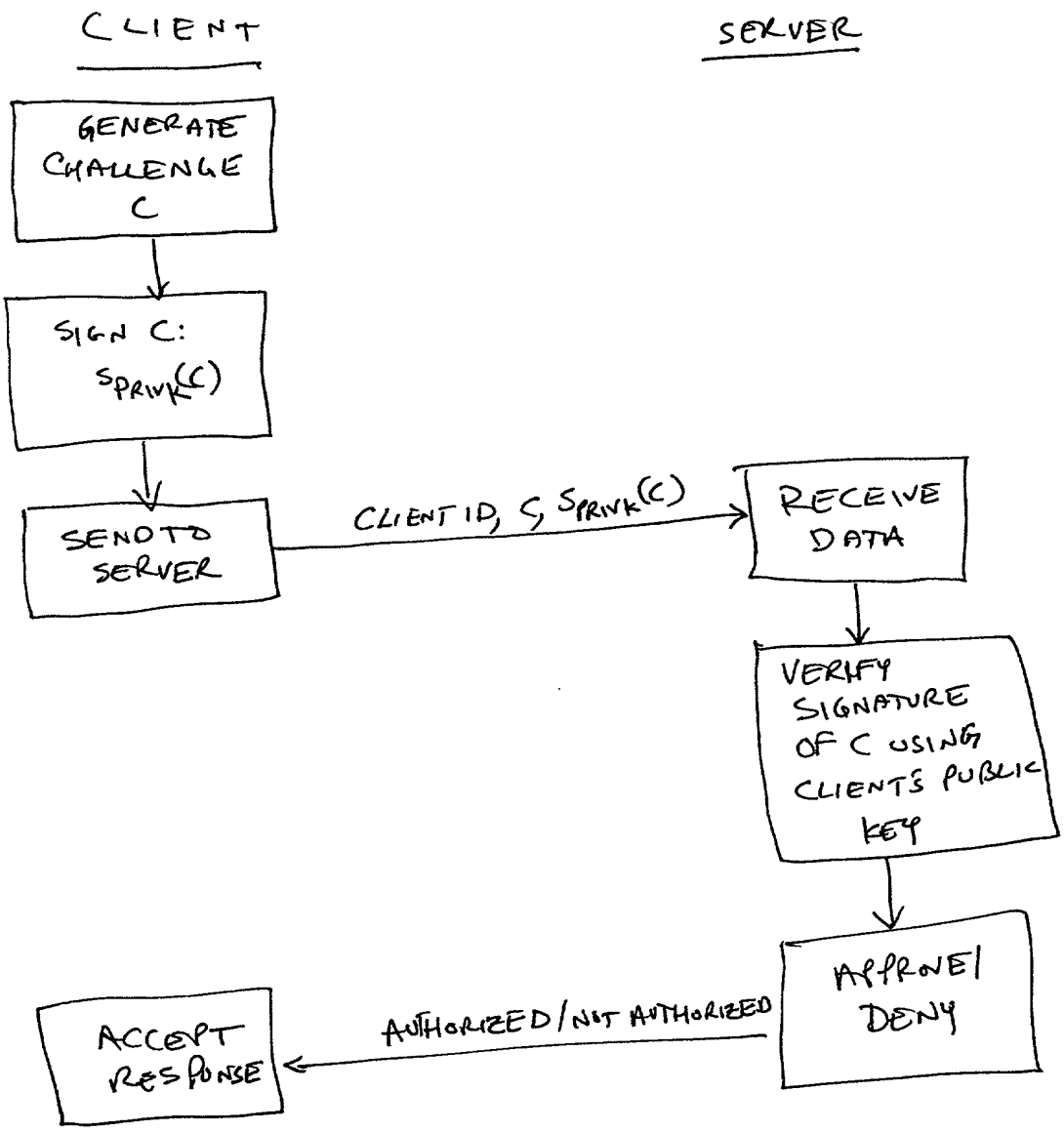
CLIENT
SERVER
GENERATE CHALLENGE C
SIGN C: $S_{PRIVK}(C)$
SEND TO SERVER
CLIENT ID, C, $S_{PRIVK}(C)$
RECEIVE DATA
VERIFY SIGNATURE OF C USING CLIENTS PUBLIC KEY
APPROVE/ DENY
AUTHORIZED/NOT AUTHORIZED
ACCEPT RESPONSE

FIG. 7

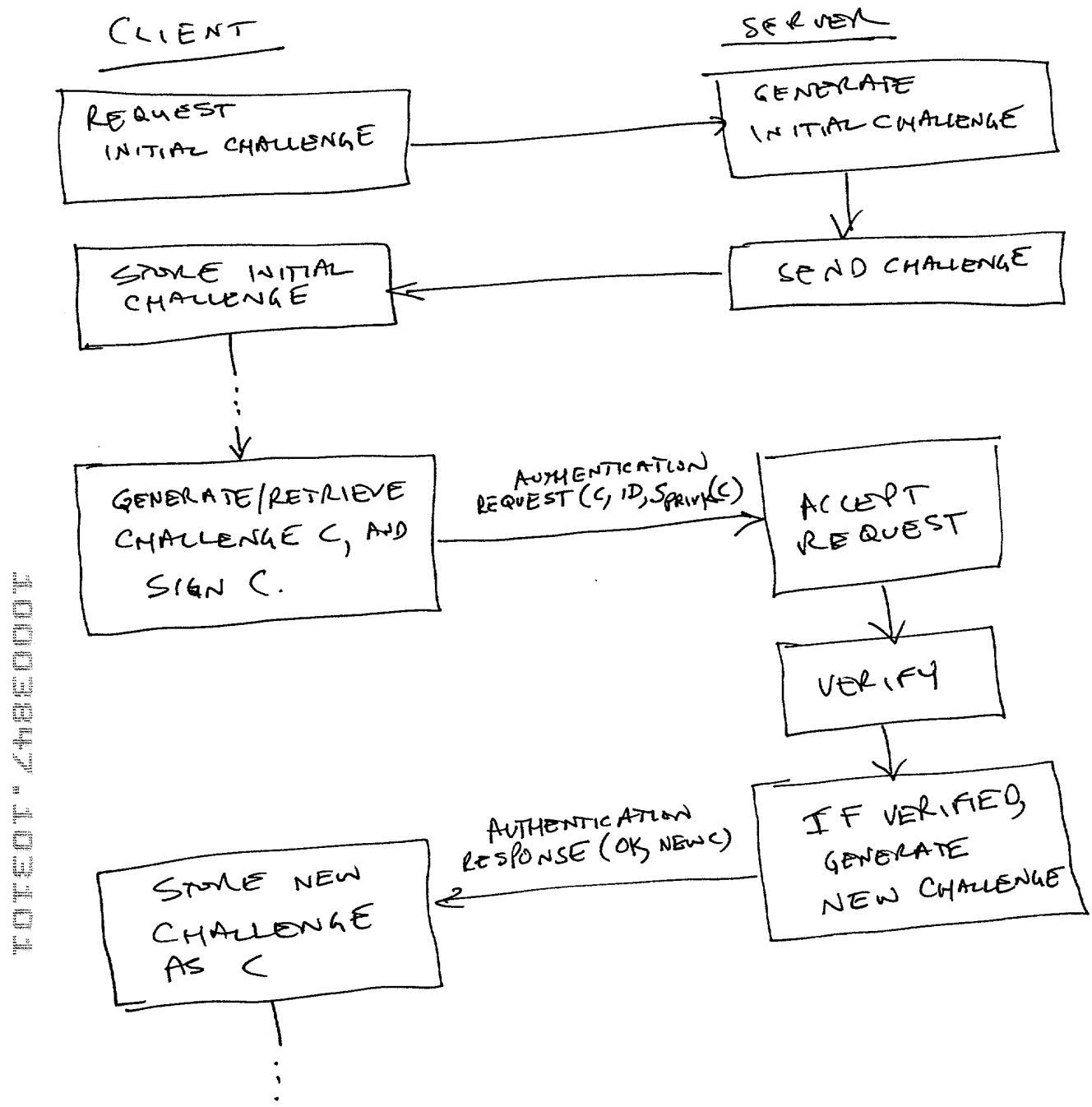
CLIENT
SERVER
REQUEST INITIAL CHALLENGE
GENERATE INITIAL CHALLENGE
SEND CHALLENGE
STORE INITIAL CHALLENGE
GENERATE/RETRIEVE CHALLENGE C, AND SIGN C.
AUTHENTICATION REQUEST (C, ID, Sprivk(C))
ACCEPT REQUEST
VERIFY
IF VERIFIED, GENERATE NEW CHALLENGE
AUTHENTICATION RESPONSE (OK, NEW C)
STORE NEW CHALLENGE AS C

FIG. 8